

pgdn

6 6 dnbd

scr lk

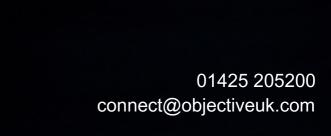
7

4

Dark Web Scanning

Understanding the Why and How.

backspad



H

8

9

0

0

P

U

Η

 \mathbf{X}

9

G

Я

D

3

5





Dark web monitoring is emerging as a crucial element of a solid, advanced cybersecurity strategy.

Unfortunately, many organisations are not aware of the dark web and its dangers.

Others don't take it seriously, thinking it can't possibly be a threat to their organisation. **Don't let your business fall victim!**



Dark web monitoring is another arrow that you should add to your cybersecurity quiver.



Today's hackers are working smarter, not harder, and they have become increasingly adept at lucrative opportunities tied to the hostage of business email. Yet many companies aren't prioritising security as an essential element to their business success.

OBJECTIVE[™] Stress Free IT

Take, for example, employee training. Many businesses don't realise their employees are one of their most significant security risks. You've probably heard the stories of cyber criminals dumping thumb drives loaded with malicious hacker code in employee parking lots, waiting for someone to pick one up and plug it into a work laptop. Pretty clever, right? Unfortunately, research studies have found that more than 60% of people who find a thumb drive will do just that - potentially handing over network access to an enterprising hacker.

Research finds that most breaches are not initially detected and may not be discovered until several months after the initial attack. According to IBM's Cost of a Data Breach Report 2020, the average time to identify and contain a data breach is 280 days (approximately nine months).

Often, breaches are only detected after it is discovered that compromised, sensitive information has been released or is for sale on the dark web.

Does your organisation have compromised information available for sale to hackers?





Do you have Employee Credentials on the Dark Web?

Today's hackers are working smarter, not harder, and they have become increasingly adept at lucrative opportunities tied to the hostage of business email. Yet many companies aren't prioritising security as an essential element to their business success.

Take, for example, employee training. Many businesses don't realise their employees are one of their most significant security risks. You've probably heard the stories of cyber criminals dumping thumb drives loaded with malicious hacker code in employee parking lots, waiting for someone to pick one up and plug it into a work laptop. Pretty clever, right? Unfortunately, research studies have found that more than 60% of people



There's no better time to find out.

Many organisations are shocked and surprised when they see their employees' access information available for sale on the dark web.

Whether you have a large enterprise or a small- to mid-sized business, be sure you aren't a target!



What to do when your credentials have been exposed.

Running a dark web scan against an email domain can provide illuminating results. For example, one organisation's email domain scan uncovered 30 compromised emails, including the business owner's bank account login credentials. Keep in mind, this is just one example.

There have been instances where several hundred or even a few thousand compromised emails have been found.

Client Report



UNTENT	Security Assessment			Patch Assessmen	et .			Risk
An Real	This security assessment report provides quelify weaknesses and definiencies in th		Vulnerability Assessment Automatily assessment's to proses of adverging	Patch assessment is the process that helps acquire, test and install multiple patches on a computer, analysing systems to stay updated on existing patches and safeguards the IT				Detecto
05 Anti-Apan	amployed within or inherited by the inform buch residences and deficiencies are pr schemeluffers. Freedoling by a firmed scare		releast infrastructures to provide the organization doing with the reconcury incodedge, awareness and risk back, understand the threads to its annitrument and react again	and one of the scherability	tes and aquitits			La
	prevaled during the security control accorring to the security of the security			Apply Patch to Sta	sy Protects	ed		-
06 Xanananan	shuckured approach to milipating taks in a organizational priorities.		Risk Detected: High Risk Score	Critical	High			D.
08 Endpoint	Risk Dashboard		Critical Severity Valuerability	Apply patches within 30 days of release	Apply parts			
10 200		10	H unique orbait seconds scherabilities was decreared. On scherabilities require investigate adjusters. They are relatively adjusters to applicit and may provide them with full context of the scherabilities.					ė
10 Assessment				Medium	Low		_	-
11 Section	RISK	23	High Severity Valuerability 2) origin high search scheduline une decoursed, high a scheduline are obschedule to exploit and may bet provide access to obschedule spaces.	Apply patches within 60 - 90 days	Apply pets 180 days	hes within		Ă
			Modium Severite Valuerability					- 43
12 Assessment	The Conscillated Real Report appropriate from multiple assessments performed on providing you with both a Conscillated R		El unique methors annuelle université entre decouverd. In schwaltifies after provide information is attachers that may ben in munitipe scherauent attachers on universit. These	Top 3 Minning Patches				
	a high-level overview of the health and a reduced.		alter fan fanal is o tinely vanmer ful are nit an organi as the of schematolites.	Page Departs	•	nating Court	-	
	The report details the steps taken to dear	65	Low Severity Vulnerability	Reads into a Manager of				
	issues. In addition to the overall Consolid the report also presents separate impact arous of assessments.	03	B) prigation anothy schemitting area decorrent. These pipe in-final is a timely improve had an out as opport as final	Security (passe for Windows 1) Saline (Hild Windows)	the de	ж	14	

Assessments

- Dark Web Assessment
- Anti-Spam Assessment
- Vulnerability Assessment
 Endpoint Assessment
- Patch AssessmentUser Risk Assessment
- IT Infrastructure Assessment

Partner Report

-		Open Vulnerability Details					Endpoint Health Details								
		-	CVB8 Score		_	_	Muchine Name	IP Address	Machine Type	Operating Byshem	Frend		DAS Protection	Remote Desktop Disabled	Open
Contents	CM ID	Vulnerability Name/Description	(Risk Level)	Endpoints	Deprecated?		SERVERI	192.168.16.2	Server	Microsoft Windows Server 2008 R2 Standard	1.1			1.1	
	CHE MINH	obe-server before 1.7.7 allows legans by unconfirmed' accounts due to a bug in the REST apr	88(1924)	SERVERI, DESKTOP2		100.00	DESKTOPS	192 198 2 8	Gestion	Microsoft Windows 12 Pro-	1		•	×	40
	CVE-2010- 3792					0000410	06547049	192 158 11 156	Canaditation	Microsoft Windows 12 Pro-					10
COntechto		Improvementation. Convension scripting (NSS) understatility in the landstand in Open-Kitherge (SK), Applicate 7.2.4 balling 7.2.2 and 7.4.4 balling 7.4.5 band/0 allows services and/over the Child Convension and and and NOTE: the understatility are SM-IT from CME-2015 4542 because II which is defined and another.		BERHERI, DESKTOPT, DESKTOPT			DESERCTORS.	192 198 18.8	Centro	Microsoft Windows 12 Pro-					_
						10.04	Delta hores	102 108 1 94	Central	Manual Westing 12 Pro-					
Anti-Spam Configuration Details						Adverse	DESKTOPE	192 108 254 10	Centro	Microsoft Windows 12 Pro-	0	0	0	0	1000
	CVE-2013-						DESKTOP7	192 108 2 8	Dealthip	Microsoft Windows 10 Pro	1			1	
ark Web Exposure Details						Mailer	Q. Could not be determined/scanned/Round.								
							Users with	Users with Possible Policy Violations Details							
ers with Possible Policy Violations Details		In fance agents before 4.0.17 data not verify remote 505, certificates in the fance, mixed, uss py script adult can pathemistry silver in reas-or-the- motifie attackers to sport 555, servers na arbitrary 556, certificates.	1.9 (MEDIAN)	DESKTOPS DESKTOPS		Man, Jan Man, Jan 2015	User Name		her Role	Last Login Timestamp	Passant I	hangeable	instanting in the second	Password Expiring in Less than Hi Days	Ramata Desiti Access Enabl
Endpoint Hygiene/Asset Details	CVE-2014-						SERVERTORING		desistation	NA	1	× .			
	1.1					200.00	SERVERTURET DESENDERTURET		lued	04/07/2020 9 18:45 PM 04/06/2020 7 53:48 PM				· ·	
Open Vulnerability Details							DESKTOPTUNE		descent of the	04060520 7 53 48 PM	1		-		
Missing Patch Details		The MHSD plugin (MHSD dl) before 4.37 for therefore allows remote allockers to execute arbitrary code via a steard log.	78(HGH)	DESK70P7	· •••	10ks./bs	SERVER Funnet		desired and	04/08/01/0 8:57 14 PM	2	2			
	CVE-2013-						DESKTOPHUND		desination	401170500 2 36-51 AM	1	*			
						1034.744	SERVER Loand			001200104181576					

Brush up on Password Best Practices.

If your credentials have been exposed publicly, you can never use that password again. Once that password is part of a public list, especially one that is associated with your email address, you can be sure it will be used in a future attack. The risk is too great to even consider using it again, and any other account that uses the same password should be immediately changed as well. Similar passwords used with other accounts should be changed, too.

OBJECTIVE[™] Stress Free IT

Cybercriminals will use your password in an attempt to gain access to other accounts like banking and social media. This is why business email addresses should NOT be used for non-business-related activities. Separate passwords should be used for each site or application you use. The results of a dark web scan will show if any of your employees may have used their business email for nonbusiness reasons and had their credentials compromised, bringing unnecessary risk to your organisation. If you identify any of your users' credentials for sale on the dark web, take the necessary steps to remediate the situation and prioritise strengthening your security posture for the future. That includes training your users on their role in defence of the organisation. While a clear dark web scan may provide peace of mind today, be sure not to develop a false sense of security. Instead, use the assessment to identify other potential vulnerabilities that require resolution.





Using a Dark Web Scan as an Early Warning Tool

Think of a dark web scan as a regular checkup with your doctor.

You may feel fine, but medical tests could uncover underlying problems. A dark web scan is just like the routine tests your doctor orders. It's one more way to understand the strength of your current cyber defence.

Additional tests, like a vulnerability scan, can further identify specific areas of weakness and recommend appropriate remediation.

